Monika Büscher, Michael Liegl, Shaun Perng, Lisa Wood

How to Follow the Information? A Study of Informational Mobilities in Crises

(doi: 10.2383/77044)

Sociologica (ISSN 1971-8853)
Fascicolo 1, gennaio-aprile 2014

Ente di afferenza:
()

How to Follow the Information?

A Study of Informational Mobilities in Crises

by Monika Büscher, Michael Liegl, Shaun Perng *and* Lisa Wood

doi: 10.2383/77044

1. Information in Crisis

"Data is the new oil," perhaps *the* most vital ingredient for recovery from the current global economic crisis [McKinsey 2011]. But as "knowing capitalism" is generating more personalized products and services more profitably [Thrift 2005], a "century of disasters" is taking shape [eScience 2012]. Population growth, migration to cities, and climate change engender greater vulnerability and more frequent and more severe natural and manmade crises. Under stress from austerity and increasing demand, crisis management is one area where data-based efficiencies are eagerly sought. In preparation for or response to a storm, pandemic or terrorist attack, data about persons and places affected can be pivotal for effective and (cost-)efficient response, and better data-sharing between emergency and other public services is high on many governments' agenda.

However, this "informationalization" of services has long been recognized as problematic. In 2006 Caspar Bowden, former Chief Privacy Adviser at Microsoft warned that "traffic data":

> "constitutes a near complete map of private life: whom everyone talks to (by e-mail and phone), where everyone goes (mobile phone location co-ordinates), and what everyone reads online (websites browsed)." [Rauhofer 2006, 323]

"Traffic," "transactional" or "communications" data are personal data[1] generated in vast quantity by all but the most marginalized people as part of everyday living with digital technologies. This "big data" [Mayer-Schönberger and Cukier 2013] has mainly been collected and aggregated by internet and telecoms companies such as Google and Yahoo, who could be seen as actually leading the field of "computational social sciences" with government agencies such as the U.S. National Security Agency piggybacking on them [Lazer et al. 2009; Lesk 2013, 86]. Yet at the same time government efforts for developing and better joining up "non-interoperable and incomparable and conflicting datasets" can be observed. For instance in the UK "joined-up thinking and government" and "connecting the dots" in databases was introduced by New Labour's "Transformational Government" strategy, which consequently was characterized as a "database government" [Anderson et al. 2009, in Ruppert 2012, 117]. Likewise the US government recently announced a Big Data Research and Development initiative [Kraska 2013; Tene and Polonetsky 2013].[2]

With growing capacity for capture, analysis, sharing and data-driven decision-making, the "seas" of such data are becoming more navigable and exploitable, increasing the risk of inadvertent disclosure or misuse of personal data. 72% of Europeans are "concerned that personal data may be shared without their permission" [Reding 2012], prompting a comprehensive reform of the EU's data protection rules, which will come into operation in 2014 [European Commission 2012]. Recent disclosures over surveillance through the US National Security Agency and the UK Government Communications Headquarters are fanning the debate [MacAskill et al. 2013]. Sociological analysis has also long warned that an exchange of personal data for more convenience, efficiency and security is a *Faustian* bargain [Urry 2007], and amongst citizens (and non-citizens!), policy-makers, politicians and academics, concerns over a crisis of information are spreading.

However, there is a dearth of studies of the specifics of data flows, intentions and practices of data processing and effects in particular contexts [Yar 2003]. In this paper we contribute to debates about a crisis of information through a study of infor-

[1] According to the EU Data Protection Directive 95/46/EC "personal data" means "any information relating to an identified or identifiable natural person ('data subject') … who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." The Directive identifies "sensitive information," such as data concerning racial or ethnic origin, political opinions, religious and philosophical beliefs, health, sexual life and criminal activities, and prohibits processing of all personal data without the consent of the data subject. However, exceptions apply.

[2] http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release.pdf (241).

mational mobilities in crises. We use the umbrella term "crisis" to draw emergencies such as large accidents, natural and manmade disasters, as well as financial crises, political unrest and riots into the frame. This is useful because data-based efficiencies can apply across a wide spectrum of crises, and the pressures that arise in crises often incite intense informational mobilities – for risk assessment, intelligence and criminal investigations, or for determining the number, status and specifics of victims, as well as causes and consequences of the crisis. Exceptional license to process personal data can apply to historical data, utilizing mandatory retention of communications, for example, during national security operations [Rauhofer 2006], and it can involve sharing of newly collected, live data between a variety of organizations (fig.1).

FIG. 1. Actors and Organisations Involved in Data Sharing in Crises

In the UK, statutory "category I" responders (police, fire, and ambulance services, local authorities, healthcare organizations, and government agencies) may exchange information with a range of category II "co-operating responders" (utilities companies, Internet, social media and telecommunications service providers, highway agencies, railway, underground and airport operators). If a 112 call is made, for example, the telecoms company will disclose the caller's location to emergency agencies. The Italian government is said to have used cell-phone data to locate Italian

citizens after the 2011 disaster in Japan,[3] and the city of Amsterdam is testing techniques to track people's mobile phones within the impact area of a chemical accident to support incident management [Steenbruggen et al. 2013]. In addition, a range of volunteer organizations such as the Red Cross and commercial organizations such as insurances, supermarkets or hotels may share information, and information is also mobilized by the media and those affected by a crisis.

It is difficult to study how information is mobilized between these diverse actors, or even what kinds of data they use. In their diagnosis of a "coming crisis of empirical sociology," Savage and Burrows [2007, 896] call for "a new politics of method" based on "a radical mixture of methods, … link[ing] narrative, numbers and images in ways that engage with, and critique, the kinds of routine transactional analyses that now proliferate." In this paper, we contribute by exploring informational mobilities in crises by "following" information in different ways. While this research is closely related to the ethnography of (digital) infrastructure and large socio-technical systems and touches on similar methodological issues such as multi-sitedness and scaling [Bruni 2005; Marcus 1995; Ribes 2014; Star 1999], in this paper we are not so much focusing on data infrastructures, but rather on data practices. For this we deploy the ethnographically minded approach of mobile methods which attempts to "capture, track, simulate and shadow the many and interdependent forms of intermittent movement of people, images, information and objects" [Büscher et al. 2011, 7]. A large part of this research observes digital data or mediated interactions such as twitter messages or "tweets," but also interviews with participants. Yet, because we draw from intimate knowledge about the field and its practices, we follow Christine Hine's forceful argument for calling it "ethnography" [Hine 2007]. We begin with a discussion of challenges and opportunities of informationalizing crisis management. These debates motivate our research, which informs socio-technical innovation for more socially sensitive and ethically circumspect mobilization of information in crises. We describe how we track, go-along with, trace, and shadow information to develop a better understanding of the practices involved, with reference to examples such as the 22/7 Norway attacks. We conclude with a discussion of alternative design philosophies.

2. Challenges and opportunities

In a recent emergency communications stocktaking effort, the European Network and Information Security Agency [ENISA 2012] shows that despite the recent trends toward data sharing, data convergence and interoperability which are

[3] Senior Irish Fire Officer, personal communication.

discussed as "Big Data" or in a governmental context as "database government" [Anderson et al. 2009], current information sharing practices between emergency agencies are often inadequate. One of the reasons identified is an "over-zealous or incorrect interpretation of the duties imposed on public organisations by the Data Protection Act" [Armstrong et al. 2007]. After the London bombings, for example, some responders deemed it to be illegal to pass on personal data collected from victims by the Family Assistance Centre to successor organizations, which complicated continuity of care. Clearly first responders are overwhelmed by these apparently contradictory demands. While these effects are clearly deleterious, sociological research shows that there are often good social and organizational as well as political reasons for separation between the different agencies [Quarantelli 1966; Drabek and McEntire 2002; Allen, Karanasios, and Norman 2013; Scheppele 2003]. In the European Union, calls for better technological support acknowledge this, at least partially:

> "We are not yet at a stage when we can envisage to interconnect information management systems from different organizations to share situation assessment or automate coordinated response procedures. For many reasons (political considerations, concern about … confidentiality..., competition or conflicting objectives between organisations, human behaviour, lack of financing, etc.) there is no willingness to establish direct interconnection, but rather a need to utilize human interfaces between systems." [M/487 2013]

But the "yet" in the above quote also indexes a strong belief in technology to overcome these frictions, to interconnect and even automate response procedures. These hopes resonate strongly with post-disaster and emergency planning reviews which often combine critique of response agencies' current lack of coordination with a vision of opportunities through better use of existing or new information and communication technology (ICT):

> "Norway 2011: More sophisticated use of ICT has a substantial potential for improving efficiency and quality … This is a key to better emergency preparedness in future." [Gjørv 2012, 20]
> "New York 2012: The City did not immediately have access to accurate, timely data …. As a result, it took a few days — and in the case of telecommunications, longer — to get an accurate, comprehensive understanding of the magnitude of power and service outages." [Gibbs & Holloway 2013, 18]
> "UK 2013: People aged 65 or over account for over 50% of all fire-related deaths … Prevention … will need to be facilitated by better data-sharing across public services." [Knight 2013, 71]

Innovation eagerly takes its cue from such critiques. But funders, technology developers, implementing organizations and researchers also recognize that a lack of understanding of the realities of organizational practices can lead to costly fail-

ures [Committee of Public Accounts 2011; Shapiro 2005]. Two projects seek to resolve some of the tensions by integrating "domain analysis" – qualitative studies of social practices of collaboration – with stakeholder engagement and collaborative design methods to design new technology. The BRIDGE project (http://www.bridgeproject.eu) is about developing computer infrastructures that can help responders assemble ICT systems to support inter-organizational interoperability and information sharing, while *SecInCoRe* develops secure cloud-computing for information, communication and resource interoperability in Europe. This research is also inspired by a convergence of "smart city" and crisis management systems, powerfully illustrated (Fig.2) by Maeda et al's vision of "Next Generation ICT Services for the Resilient Society" [2010] in Japan.

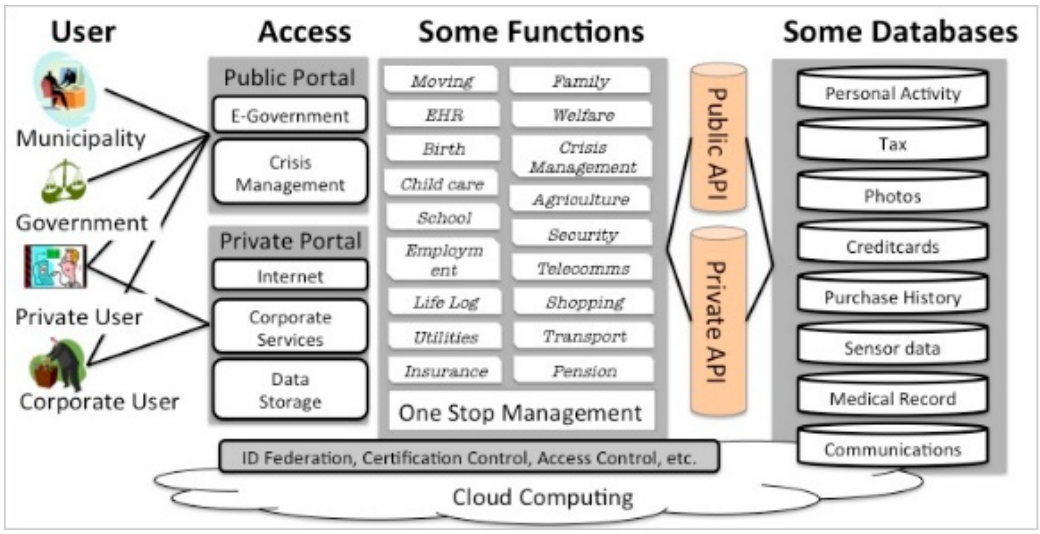

FIG. 2. Next generation ICT for the resilient society
Source: Adapted from Maeda 2010

Such computer architectures can enable "one stop management" of datasets ranging from personal activities (diaries, location, photographs, blogs) to employment, taxation and health records, telecommunications and risk registers. Researchers, organizations and governments in Brazil [Naphade et al. 2011], the Netherlands [Steenbruggen et al. 2013] and the UK [Johnson 2012] are extending similar "one stop management" to security and crisis management. In the European context interconnections between legislative and executive agencies are governed by strict rules, but secure information sharing that respects these rules (or is exempt through exceptions) is seen as an important area for innovation.

However benignly intended, increasing information sharing poses challenges. It is not clear how "secure" direct interconnections, respect for rules and responsible

exception management can be supported with the technical, organizational, political and legal means that are being developed. In fact, eager embrace of technological advances in everyday life, commercial and civic organizations has so far brought unprecedented levels of surveillance and an erosion of democratic values and civil liberties [Crang and Graham 2007; Lyon 2002]. The social sorting that becomes possible with traffic data can splinter societies [Graham and Marvin 2001] and allow exceptions to spread [Agamben 2005; Scheppele 2003]. The all-pervasive focus on risk and security creates fearful societies [Aradau, Lobo-Guerrero, and Van Munster 2008], fostering the enactment of a pervasive securitization of mobility [Amoore 2006; Adey 2009]. Some analysts observe a militarization of everyday life [Graham 2008] and the development of a "culture of fear" [Furedi 2006], resulting in life "lived as the continuous emergency of its own emergence" [Dillon and Lobo-Guerrero 2009] subject to increasingly comprehensively enforced preventative measures in healthcare, justice and disaster management [Amoore 2011; Brown and Adams 2007; Tulich 2012]. While some surveillance studies evoke Orwell's "Big Brother" as a metaphor to characterize the dangers, many highlight more "disorganized" forms of surveillance, where many actors rather than one centralized bureaucracy, collect and share data in ways that are hard to fathom [Lyon 1994]. Daniel Solove [2004] highly effectively evokes Kafka's novel *The Trial* to capture the surreal anxieties, violations, and anxious governmentalities that an erosion of informational self-determination in this landscape can engender.

What should designers, practitioners, politicians, policy makers, researchers, and (non-) citizens do? A curbing of informationalizing innovation for knowing capitalism is unlikely in many societies worldwide [Urry 2013], and the twin pressures of financial cuts and an increase in disasters make it highly improbable in crisis management. With reference to information technology, "Don't do IT" may be a sound conclusion to draw from surveillance studies, but it is not easily practicable. "Do IT more carefully" could be a better maxim, but to specify what "more careful" might mean, there is a need to better understand how information is mobilized and shared in crises.

3. Following the information

"Information" is a situated and relational concept – what constitutes available, relevant, important or unimportant, sensitive or "shareable" information differs for different persons, times and contexts. As a result, information is not a pre-existing entity, but a phenomenon *in formation*, performed in people's interactions. To de-

velop technologies that can support information sharing, people's practices of noticing and defining information, reasoning about and with information, and acting on information must be better understood. When we talk of "mobilizing information," we refer to all of these activities. In this section we present excerpts from different strands of analysis from studies of information practices to explore methods of and insights gained by "following the information."

3.1. Tracking Information

What we call "tracking information" involves following information "on its heels" either live, as it happens, or through "rapid response" fieldwork. The aim is to develop a better understanding of the formation of information as this is practically achieved in and through people's actions. It often begins in the midst of breaking news.

> Lancaster, 22nd July 2011. Car Radio:
> BBC Radio 4 speaker: (let me turn to)[4] Knut Amundsen, a minister in the Norwegian government.
> Amundsen: ((speaks breathing and sighing heavily)) As you can imagine by looking at the TV, this is from Oslo, this is a situation as chaotic as possible to imagine or indeed not possible to imagine. So by now we are trying to stay focused and we are focused on the rescue operation, errm, the injured and that is our focus by now and then we take everything step by step.
> BBC Radio 4 speaker: Let's join Lars (inaudible), a Norwegian journalist with particular interest in terrorism and security. Political violence is virtually unheard of in Norway isn't it?
> Lars: It is. But before I come to that, I can bring you some breaking news as well. There are several Norwegian media, including the state broadcaster are now saying there have been shooting at a gathering of the youth wing of the Norwegian labour party …
> (Transcript from audio recording, 17:09:42 British Summer Time, 22.6.2011)

On hearing this broadcast, one of the authors pulled into a lay-by, and contacted our colleagues in Oslo. When they replied that they were okay, she asked them to capture data (media, social media, official reviews). The following excerpts from our analysis of this data allow some insight into the process of tracking information for a richer understanding of how people mobilize information. We begin with an account of what happened constructed.

[4] Single brackets indicate that we are not sure what was said due to the quality of what can be heard. Double brackets provide additional information, for example about intonation or context.

> "At 3:25 on 22 June 2011, a Friday afternoon, a bomb went off in the government quarters in Oslo. The emergency response call centre was immediately overwhelmed with calls. Images of bleeding victims were shown in the news. A number of hashtags emerged on twitter, gathering eyewitness reports and helpful information, such as numbers to ring to find out about missing relatives.[5]"
> Shortly after the explosion, Anders Breivik (ABB) drives from Oslo to Utøya, some 40 km northwest. He leaves his car and gets a ferry to the island, where he starts shooting people, dressed as a policeman at 5:21.

The first reports about the shooting emerge on Twitter at 5:41 pm Norwegian time (CEST), 12 minutes before the first newspaper reports.

> By this time, police and ambulance services have been alerted, and the police arrive at the ferry port at 5:52. But they relocate to the more distant Elsetangen and arrive on the island at half past six, when they arrest Breivik.
> (Description constructed from media reports and twitter data)

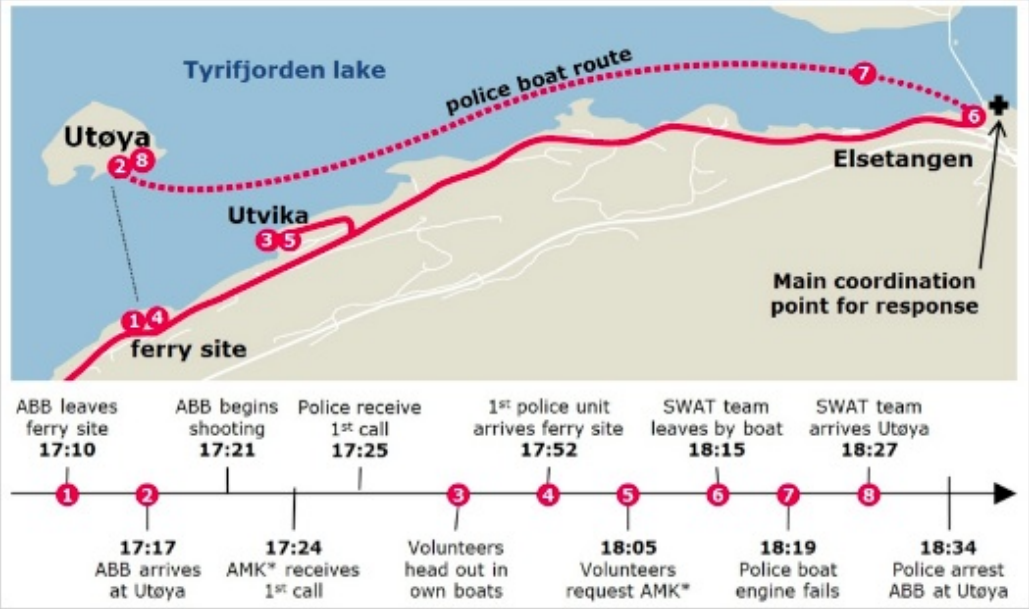

FIG. 3. Simplified overview of the coordination of rescue personnel around Utøya. *AMK is the Norwegian Ambulance Service.

Source: Picture redrawn from Aftenposten, 12 August, 2011 by Ragnhild Halvorsrud and Michael Stiso, reproduced with permission.

[5] By embedding hashtags, such as #osloexpl #norwayterror #bombeoslo into their twitter messages, people enable others to search for messages related to particular events or topics.

FIG. 4. First Reports about the shooting on Twitter[6]

Source: Gjørv, 2012.

Amongst the data we collected and analysed on 22nd July 2011 and the months after are around 220,000 tweets. We used a grounded theory approach [Corbin and Strauss 1998], where several researchers read the tweets and derived categories of phenomena. One particularly interesting category was loosely termed "mobilizing help," and it was inspired by calls for help or examples of assistance provided, such as the helpful telephone numbers mentioned above. Amongst the tweets tagged into this category, we found this:

> "@cTee tweets @NilsPetter:[7] We are sitting by the lake. A man dressed in police uniform is shooting. Help us regarding when the police will arrive." (5:58pm CEST 22nd July 2011, from Twitter for iphone)

At the point this message – providing and requesting information – was sent, the police had already been at the ferry pier, less than a mile away across the water, for six minutes. However, as figure 3 shows, it took them more than half an hour to get to the island. We will discuss some reasons below, but finding this message led us to track related information. We visited NilsPetter's profile, and found a stream of updates from the island.

[6] Twitter names and some details from tweet texts (preserving the content) have been changed to help protect people's anonymity. Several have been translated from Norwegian.

[7] Throughout this paper, names and place names have been changed, and where visuals are used, faces have been obscured, to protect the anonymity of participants.

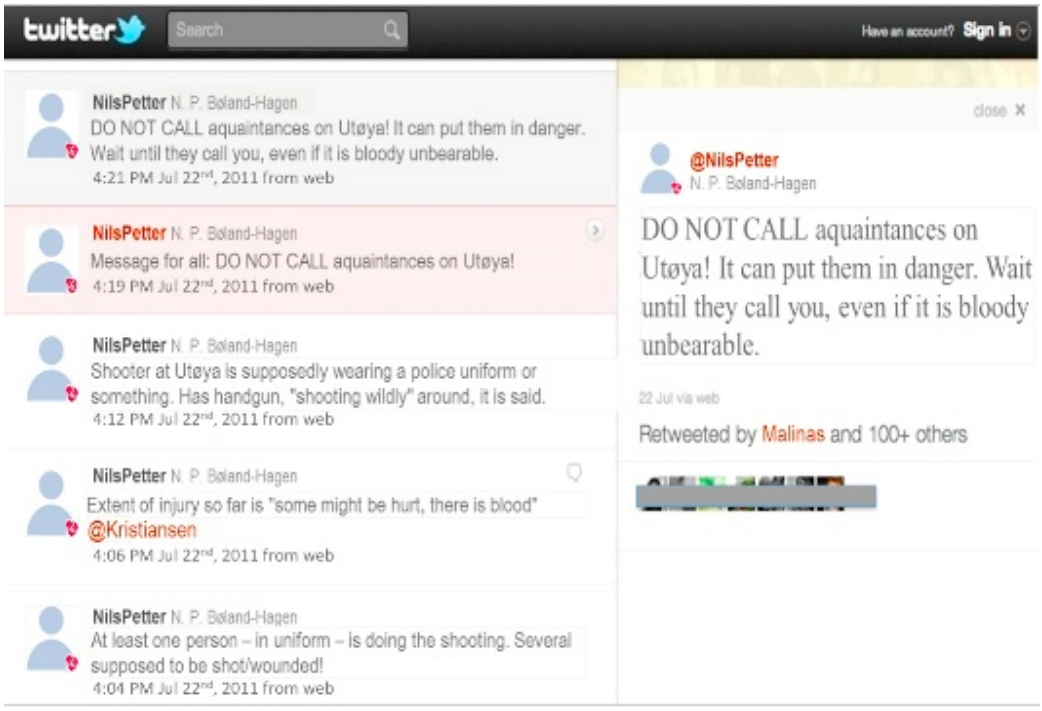

FIG. 5. Tracking Information on Twitter

When the figure 5 is read from the bottom up, it becomes obvious that NilsPetter received frequent reports about the unfolding situation. His messages at 4:19 and 4:21 document the formation of a keen awareness of danger. They clearly struck a nerve and were immediately retweeted or forwarded over one hundred times. The latter message finally had 281 retweets, many from persons with several hundred to over 8000 followers.

Some of the residents and tourists nearby the island heard shots and cries for help and used their boats to pick up people from the water. In parallel, numerous tweets and mobile phone messages encouraged this mobilization of local resources:

> "Boats on Utøya are recommended to pick up people from the water. The temperature is low .. High risk of drownings .. Rescue boat is on the way." (Via Twitter)
> "RT @elisefang: do you have a boat close to #Utøya? Pick up swimming children around Utøya! #osloexpl #norwayterror # bombeoslo." (via Twitter)
> "You have to get in the boat … and rescue people from Utøya, because something terrible is happening there." (Via mobile phone) [Watkins 2011]

Using personal digital devices, people caught in the midst of a crisis increasingly use social media to publicly document events and needs, to comment on the official emergency response efforts, or to self-organize or "crowdsource" help (such as search and rescue or clean-up operations). This can be problematic. During the 2008 Mumbai attacks, information disclosed on social media was used by the terror-

ists, jeopardizing the "information superiority" and safety of responders [Oh, Agrawal and Rao 2010], and rumors can spread fast on Twitter. Much of the existing research focuses on facilitating transactional analysis to develop or evaluate techniques for rumour detection, sentiment analysis and crowd control [Castillo, Mendoza and Poblete 2011; Cheong and Lee 2010]. But following the information by tracking it can also highlight positive contributions [see also Vieweg et al. 2007]. In the Norway example it is difficult to establish a link between information ("It can put them in danger," "High risk of drownings," "Rescue boat on its way," "something terrible is happening") and action. Establishing whether members of the public stop calling or proceed to help in direct response to information provided via tweets or texts requires further research. However, the fact that reports and requests were made in significant numbers through different channels simultaneous with volunteer rescue action suggests that new practices of "micro-coordination" are emergent. Ling and Yttri [2002] analyze how people coordinate everyday activities such as shopping or meetings using mobile technologies. They describe this as micro-coordination, because it involves fine-grained coordination of people, places, times and objects. Our observations suggest that people are translating such practices from everyday contexts to crisis situations. An important part of this is coordination through "remote operators" such as NilsPetter, or more semi-professional volunteer virtual "disaster desk" operators [Starbird and Palen 2013]. Tracking information shows that virtual volunteer activities are at least beginning to overlap with the mobilization of physical resources and on the ground volunteers. We describe this as "peripheral response," highlighting how crises may be noticed, read and responded to by a diversity of actors, including local and potentially globally distributed volunteers, which could increase response capacity by mobilizing local resources (such as private boats). Peripheral here does not mean unimportant or "spatially distant," it means "out of focus" but critical for orientation and effective action in a complex field, taking its cue from the role of peripheral vision in human perception [Perng et al. 2013]. Statutory emergency response agencies "do not yet know how to tap these new collated information resources and the workforce behind them" [Starbird and Palen 2013], despite their potential for "rapid, highly localized assistance" [*ibidem*] and "agile response" [Jefferson and Harrald 2007; Perng et al. 2013]. More contextual understanding of informational mobilities in crises, enabled through following the information, can, as the next sections will show, illuminate why this is difficult and – perhaps – help develop such potential.

4. Information In Formation: A Retrospective Go-Along

Much of the communication delineated above was happening while the official responders were trying to coordinate a response and get the police to the island. What information was being generated and what was unknown for them? We interviewed a number of responders who were involved in the Oslo and Utøya disaster response just a few weeks after it happened. These were "critical incident interviews" [Mendonca 2007], where we asked the participants to take us through their day, tell us what they knew when, how they came to know it, who they communicated with and what they did.

In a two hour interview, Helle, an air ambulance doctor, described how he and his colleagues were alerted to the events by watching TV at their station. They called the emergency call centre to ask why they had not been requested to help. The dispatchers had assumed that air ambulance services were useful in open country and on roads, not in an urban context. However, the air ambulance crew are trained doctors and also have vehicles. They drove to Oslo and helped injured victims there, but then they were called to Utøya. On the way, they were told to stop some 15 miles from the island's ferry port:

> "When we were standing up at Sollihøgda (waiting for instruction on where to set up a reception area for the injured from Utøya), a lot of persons came with private cars and the press came, and they wanted to interview us and they wanted to know what we knew and lots of the publics, persons coming there they had children on Utøya and they had contact with them on their phones and got SMS's. Like, I'm shot and I'm dying and I am sad we been quarreling so much, stuff like that. … and also people coming from Utøya that had been evacuated and were driving back to Oslo. … they stopped and asked us 'why aren't you going to the island? It's okay now and ..', but it was never said from the police that it was secure, because the police I think, they didn't, as I or anybody else, they didn't think that this was a one man show. So if you caught one, where is the rest? I don't think anybody imagined that one man did all this. So it (the island) was never (declared) secure." (Interview August 2011)

Going along (retrospectively) into this particular situation with Helle provides a sense of the pressure and helplessness experienced by an immobilized emergency medical staff as well as the power of command and control approaches to emergency response, highlighting some conflicts. On the one hand, victims and members of the public on and around the island are providing precise reports about the situation, including information about the shooter. Members of the public are rescuing victims from the water with private boats, and people are asking the ambulance staff "why aren't you going to the island, it's ok now?" On the other hand, responders are acting within a command and control division of labour where the ambulance personnel

have to wait until they are instructed to proceed to a safe location and treat victims that are transported there (by fire and rescue teams). This instruction should come from the police, who have been trained to be prepared for secondary attacks on emergency responders and evacuees. The shooter left his car at the ferry terminal and Helle explains that there was fear that it may contain a bomb, prompting the police to abandon the ferry port and head for the more distant Elsetangen, whilst holding off defining a safe area for emergency medical response.[8]

Going along with responders with the help of reflective accounts draws out that there are conflicting information models and sense-making practices. Members of the public and often also the media establish reliability of information on the hoof, and understand the situation with a view to what action should be taken. The second model, that of the professional emergency responders, requires more circumspect verification and situation awareness [Endsley 1995], anticipating implications of action (or inaction) and developing awareness of hidden, complex and potentially cascading effects.

To understand how information is mobilized in practice here, real-time go-along participant observation would be useful. However, disasters are unpredictable, highly pressured settings; researchers could easily get in the way. To gain some insight into real-time sense-making, researchers accompany emergency personnel on routine call-outs [Landgren 2005], they "go native," for example, by training to become dispatchers [Whalen 1995], or study practices in exercises. We develop these mobile methods as part of a "follow the information" approach, but before we discuss how, we trace intersections between the informational mobilities described so far and the processing of personal data, which become visible in our efforts to follow information by tracking its mobilization with the help of post-disaster reviews.

4.1. Tracing Information

After the immediate response to a disaster, recovery, and a review of response performance and emergency plans begin. Committees of experts are assembled to analyze physical evidence, logs, recordings of communications, media resources, reports and statements from individuals to identify successes, failures and responsibilities. One example from the review of the Norway attacks is particularly interesting.

[8] Concerns over a secondary attack were only one reason for the delayed arrival of the police on the island. There has been severe criticism of the police [Gjørv 2012] and some procedural changes have been implemented in new training exercises that now allow emergency medical staff to enter the site of an attack alongside the police to start treatment in "secured areas."

Just ten minutes after the explosion in Oslo, at 15:35, a call was received in the emergency call centre. The caller blurts out a lot of information, including a car registration number, and the dispatcher requests clarification:

> Call Taker: Just tell me briefly what did you see?
> Caller: I saw what I thought was a policeman, but then I was surprised, a man with a protective helmet and police clothes and a drawn pistol who came up behind me, near the government building. I was surprised that he was walking alone and I just followed him out of the corner of my eye. Then he got into a car, a grey van with the following license number …
> (Transcribed from oral presentation of the report: 31 minutes) [Gjørv 2012]

The call taker realized that this information was important. She wrote a postit note and took it into the control room, marked as important. But the note was not noticed until 20 minutes later in what was a very busy control room. And even when it was found, it was not sent out over the radio, and neighbouring counties were not notified.

The report asks "Could things have been different, if this tip-off had found a more interoperating police force?" and to explore "whether the assumption that an immediate forwarding of the information could have stopped the Utøya attacks earlier is more than speculation," the commission correlated recordings of the GPS tracks of ABB's getaway car with the locations of police vehicles in the area, assuming that officers in these cars could have stopped the driver if an alert had been sent out. The experts find that:

> "Breivik (large dot) passes a police vehicle (small diamond) close to the American embassy (in the centre of Oslo) as early as 15:41. At Lusaka, he passes an out of town police car at 15:57, and at 16:03 he has just passed the police station at Samvika." (From oral presentation, 33 minutes) [Gjørv 2012]

Vehicle registration and live GPS data could have been instrumental at this point, but "the technical systems both for notification and for sharing information were very poor" (33:52 minutes) [Gjørv 2012]. The report concludes:

> "The authorities' ability to protect the people on Utøya Island failed. A more rapid police operation was a realistic possibility. The perpetrator could have been stopped earlier on 22 July." (English version:11) [Gjørv 2012]

Our "review of the review" allows us to trace not only how information was recognized as important, and how it was mobilized, but also to witness a broader transformation of information. The report's experts examine not only what *was* known to the emergency responders, but also information that *could have been known* and correlated. Such technological imagination is a critical force not only in post-

facto critique, but also in the formation of what constitutes available, relevant and legitimate information. Indeed, by tracing informational mobilities retrospectively, post disaster reviews also prospectively trace socio-technical futures onto the drawing boards of policymakers, politicians, practitioners and technology designers.

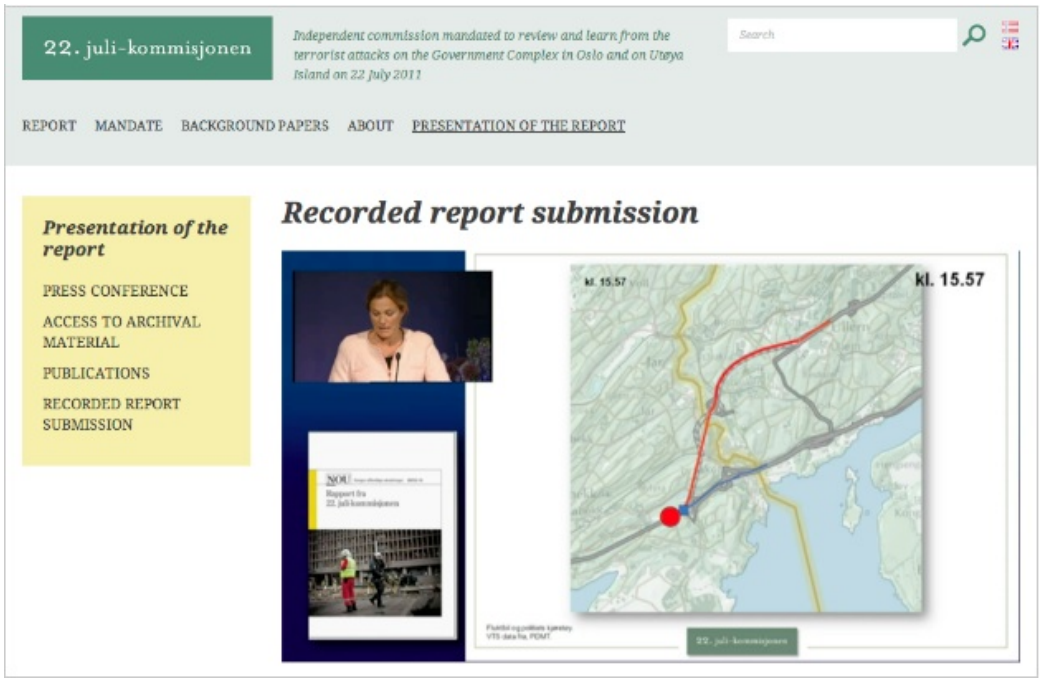

FIG. 6. Tracing what could have been known.
Source: Screenshot from http://tinyurl.com/o59sjah

The Norwegian experts are not alone in considering data about people's movements for a more integrated crisis management team, and some of their fellow travelers are ahead in implementing convergence between "smart city," big data and crisis management systems. In his 2012 re-election manifesto, Boris Johnson, mayor of London, promised:

> "Ensuring strong protections against misuse, I will extend this approach [Automatic NumberPlate Recognition (ANPR)] by requiring Transport for London (TfL] and The Metropolitan Police service [Met] to assume joint responsibility for TfL's ANPR camera system which is used for the operation of the congestion charge and the low emission zone. This would give the Met straightforward access, with an explicit purpose of crime prevention and detection." [Johnson 2012]

In 2007, similar ideas attracted 1.8 million signatures in a petition and strong criticism from pressure groups and politicians, including now deputy UK prime minister Nick Clegg, who then said that the plans exposed "a disingenuous attitude of

ministers towards public fears about a creeping surveillance state" [Johnston 2007]. Recent revelations about data retention and sharing pursued by the UK Government Communications Headquarters (GCHQ) and the US National Security Agency (NSA) dwarf these concerns. Revealing the ultimate ambition of this collaboration during a visit to a joint communications monitoring station in the UK in 2008, Lt Gen Keith Alexander, head of the NSA, asked "Why Can't We Collect All the Signals, All the Time?" [MacAskill et al. 2013]. A "collect-all" policy could create a live imprint of "the haystack," that is, all ICT supported communications (in the world), to find "needles" – terrorists and organized criminals with malicious intent, whose communications patterns are exceptional enough to "trigger" scrutiny. This is deemed necessary because terrorists may hide as "one in a million" in amongst ordinary people [Crang and Graham 2007; DSB 2004]. There is a benign impetus, as a GCHQ source reveals:

> "We have a process that allows us to select a small number of needles in a haystack. There are certain triggers that allow you to discard … a lot of data so you are just looking at needles. If you had the impression we are reading millions of emails, we are not. … The criteria are security, terror, organised crime. And economic well-being." [MacAskill et al. 2013]

The informant adds "The vast majority of the data is discarded without being looked at … we simply don't have the resources." Earlier calculations of the data volumes involved do shed doubt on the feasibility and efficiency of such screening programs:

> "If all the traffic data covered by the [2006 EU Data retention] proposal did indeed have to be stored, the network of a large Internet provider would, even at today's traffic levels, accumulate a data volume of PE 20 - 40 000 terabytes. This is the equivalent of roughly four million kilometres' worth of full files, which, in turn, is equivalent to 10 stacks of files each reaching from Earth to the moon. With a data volume this huge, one search using existing technology, without additional investment, would take 50 to 100 years." [Alexander Alvaro, MEP, in Rauhofer 2006, 340]

But Edward Snowden's whistleblowing revelations show that in 2013 analytic tools such as *XKeyscore* make analysis of volumes of data of this magnitude possible [Gallagher 2013]. The technology enables live capture of up to 75% of internet data for certain "trigger" criteria, such as "one end foreign" connections between people in the home country and abroad. But the capabilities of these systems are limited, undermining claims to be able to clinically focus only on "needles." To analyze the "haystack," search has to "go shallow," that is, apply broad rules for selection, which means the "probability that information is being collected that is unrelated to people

the NSA is really interested in (and who the agency has FISA warrants and National Intelligence case files for) is fairly high" [*ibidem*].

Yet even if capacities to analyze the "haystack" for "needles" more adequately were available, there would be questions about the quality of the haystack, and the meaning of analysis. For "Big Data is not self-explanatory" [Bollier 2010, in Boyd and Crawford 2012, 13]. Neither is big data necessarily good [Lesk 2013, 87] or complete data [Boyd and Crawford 2012][9]. Furthermore, many techniques used by the state and corporations in big data analysis are based on probabilistic prediction, which brings "profound ethical dilemmas" [Mayer-Schönberger, in Heaven 2013, 35]. Some experts are now "less worried about privacy and more worried about the abuse of probabilistic prediction" [ibid.], because probabilistic techniques of triggering scrutiny are based on processes that are alien to human reasoning. Dynamic machine learning and the amount of data processed can make it impossible for people to understand why certain persons or phenomena are highlighted as "of interest." Some such techniques have been found to be deeply racist or otherwise discriminatory (a reflection or worse, an amplification, of such tendencies within societies). Yet, they "are beginning to influence every region of life" [Heaven 2013, 35; Introna 2007]. If crisis management decisions are based on such techniques, decisions are partly made not with but *by* technologies people do not (and arguably cannot) understand.

Apart from the fundamental question of whether security, terror, organized crime, and economic well-being warrant such exceptional measures and data processing techniques, two further dilemmas arise around efforts to informationalize crisis management through integrating information systems. Firstly, using data from commercial or municipal systems for crisis management constitutes "function creep." This is especially problematic, when data from several sources is merged, "re-identifying" anonymized data and associating it with specific individuals [Tene and Polonetsky 2013, 257]. Systems that were democratically accepted for the purpose of traffic management, such as the congestion charging system in London, or the provision of communications services, as in the case of mandatory data retention [Rauhofer 2006], may now be used for criminal and security screening purposes. Secondly, the greater

[9] These concerns apply not only to the analysis of big data for state surveillance or commercial purposes. There are claims that we have reached "the end of theory," because big data analytics are said to be able to reveal patterns more effectively than theory [Anderson 2008], but apart from misconceiving the nature of scientific reasoning, such assumptions are undermined by uncertainties about the completeness and accuracy of data. When analyzing social media data, for example, most researchers do not have access to the "firehose," which contains all public tweets ever posted, but only to a "gardenhose" (roughly 10 percent of public tweets) or a "spritzer" (roughly one percent of public tweets). In regard of these limitations, Boyd and Crawford [2012, 669] argue that "Without taking into account the sample of a data set, the size of the data set is meaningless."

emphasis on prevention that arises from the potential of the "one stop management" of big data could have consequences for civil liberty and democracy, because whilst allowing states to attend to their duty to "provide security for *bonafide* citizens," data retention and analysis also allow "measures that are preemptive, exclusionary, and pay scant regard to procedural proprieties" [Zedner 2010, 379]. Such measures can "create a caste of outlaws and aliens whose status renders them suspect aside from any wrongdoing; whose interests are compromised in the name of protecting the public" [*ibidem*].

Tracing how information is mobilized through a review of enquiry reports and revelations by whistleblowers enables a better understanding of how (and which) datascapes are currently inhabited, often with much friction, but sometimes also with great secret freedoms. While information often does not flow easily at operational levels between the agencies involved in crisis management, it can be mobilized seemingly freely at the level of intelligence by secret but potentially large groups: "a total of 850,000 NSA employees and US private contractors with top secret clearance had access to GCHQ databases" [MacAskill et al. 2013]. Besides, tracing information also shows how datascapes are being shaped in technological imaginaries, more often than not with a focus on *removing* barriers to data use.

5. Shadowing

At the same time, real world practices of mobilizing information in crisis situations are often friction-rich and by contrasting these with ambitions to create open "collect-all" "data oceans" at intelligence levels, we can open up opportunities for alternative socio-technical imaginaries and design philosophies. Shadowing information draws attention to the real world practices of mobilizing information and can reveal frictions. It involves following the real-time movement of people, objects, ideas, information. This is difficult because information is multiple, it can shape-shift – from visual perceptions into verbal reports, post-it notes, digital data – and go where researchers cannot follow. Mol and Mesman [1996], in their study of orderings in a neonatal ward, ask:

> "What about the pieces of paper that travel from the ward to the dispensary? J couldn't enter the hospital's postal system with them, for its plastic tubes were … far too small for human bodies." [Mol and Mesman 1996, 422-423]

How much smaller the circuitboards of a computer! However, shadowing information even in piecemeal fashion, witnessing where it surfaces and going along as far as one may, can be productive. Indeed, the strategy to "follow the information"

arose for us during participant observations at a major crisis management training exercise designed to develop command and control procedures and interoperability between different agencies in the UK. The excerpt from ethnographic field notes below captures the moment this approach took shape. Gathered in one large room, 30 police officers, firefighters, medical personnel, local authority, and media staff were given the task to coordinate a response to an unfolding, multi-sited shooting incident. They are gathered around 10 separate tables:

> "Each table has a sign for the agency that is meant to be located there. It suggests that agencies will remain at their tables. This isn't what happens for fire and police especially, but some agencies never seem to move; media, for example, and A-District health authority. … someone tells me that the CONTEST (counter terrorism police strategy) group are in the room where we had lunch … People are sharing pleasantries, but somehow the exercise seems to emerge from this. I don't see the first 'inject'[10] being handed out but learn later that it was given to the A-District police control room … – the exercise has started!"
> "Moving about the room is difficult. There are too many people and there is a constant 'clash' of what people are doing – sitting drinking coffee or talking with a colleague. At first I don't know what these conversations are, and how appropriate it is to record them but then I see an inject being handed to a group of police officers at the end of the large central table (the A-District police control room). I head over and decide to 'follow the information'."
> (Lisa Wood, Fieldnotes 24th April 2012)

In Figure 7 and Figure 8 we capture some aspects of this strategy, show why information was difficult to follow but how this approach still allowed some insight into practices of "information formation" and sharing and the friction-full context of interoperability in crises. Two "injects" have already been handed out, describing the shooting. The A-District police control room commander (PO2) now reads out "inject3," which informs his colleagues (Police Officers PO1 and PO3 and special Firearms Officer FA1) that Armed Response Vehicles have been dispatched (ARV).

[10] "Injects" are pieces of paper that contain information about the fictitious incident used in the training exercise. They detail events at the incident scene and are designed to trigger certain responses. In this case, the injects also contain direct questions about correct interoperability procedures.

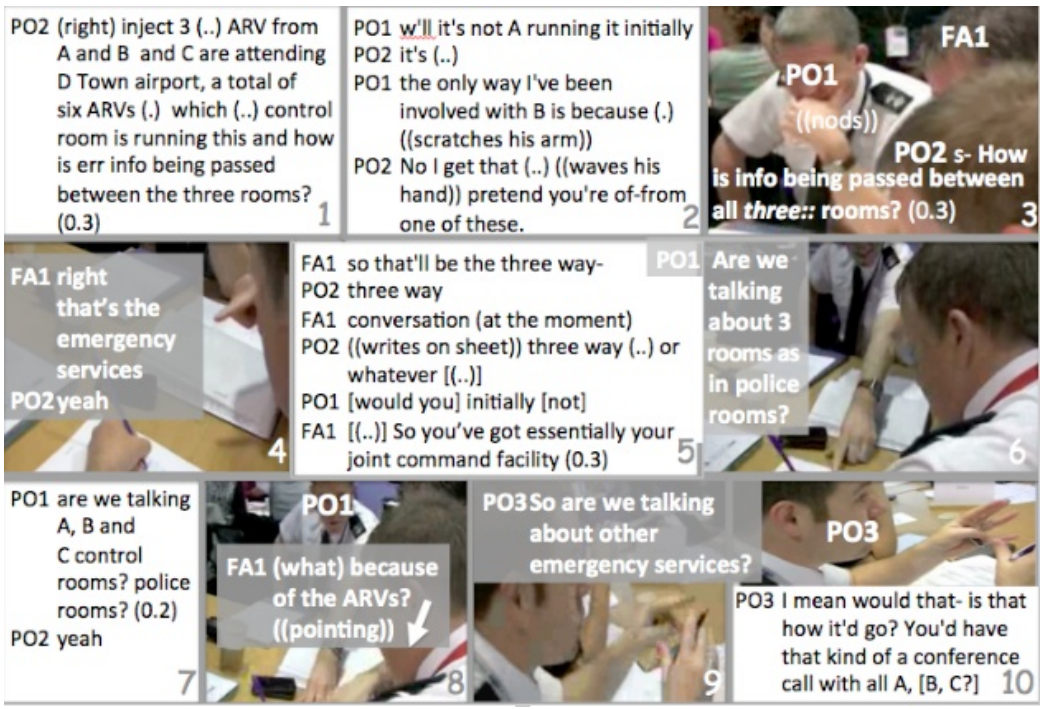

FIG. 7. Are we talking emergency services?[11]

The police officers are treating the injects like "exam" sheets, not focusing on the situation report, but the procedural questions. This brings home that the exercise is – amongst other things – a test of their knowledge of standard procedures and emergency plans. But PO1's attempt to reason about "who should be running this" (Figure 7:2), into which he tries to fold information about his personal role and career, is cut short by PO2, who is more interested in the second question on the inject, "How is information passed between the *three::* rooms?" (Figure 7:3). This prompts FA1 to suggest that "that's the emergency services," that is, the police, fire and medical services" control rooms (Figure 7:4). This would be standard procedure, and it is phrased like an answer to an exam. PO2 writes onto the inject sheet (Figure 7:4), labeling it out loud (along with FA1) with professional terminology - "the three-way conversation or whatever," "joint command facility" where police, fire and emergency service leaders would gather (Figure 7:5). But PO1 queries this, pointing at the inject: "are we talking about 3 rooms as in police rooms?" (Figure 7:7). The fact that ARV are arriving from different police force bases in A, B and C, could make a conversation between the three different police control rooms necessary (Figure 7:8). PO3 repeats: "are we talking about other emergency services?", but then also

[11] Transcription conventions: [square brackets] = overlapping speech, *italics* = emphasis, long:: = stretched sounds, (0.3) = three tenths of a second pause.

questions whether a conversation between the three police control rooms in A, B and C Districts is needed (Figure 7:9 & 10). Before the uncertainty can be resolved, the exercise coordinator (EC) interrupts them (Figure 8:1).

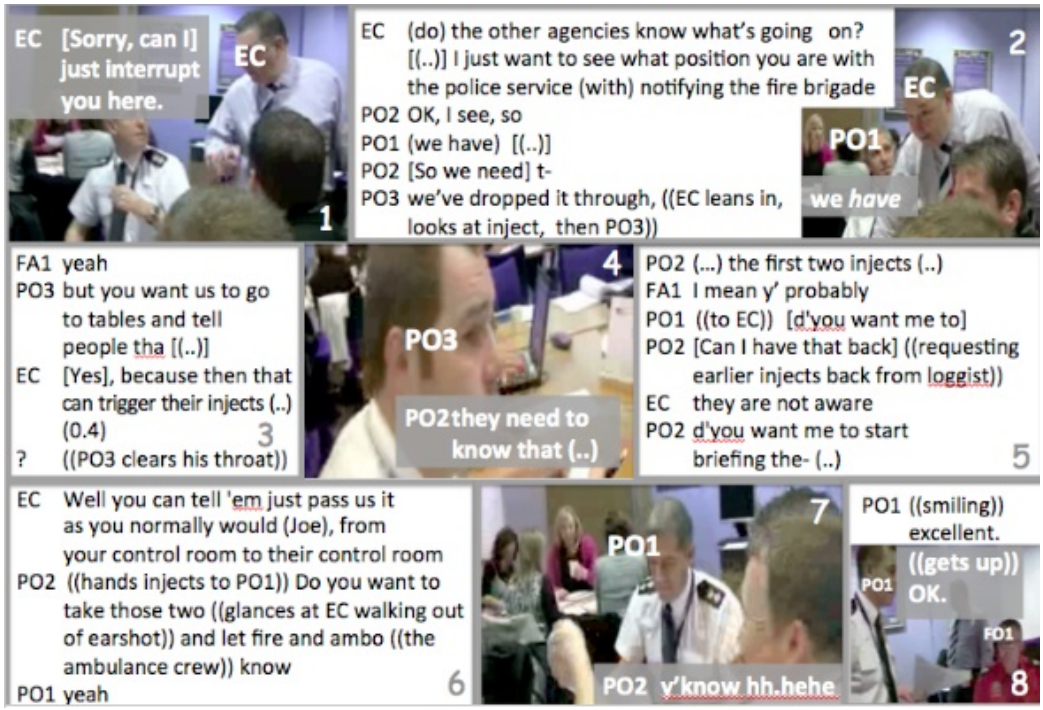

FIG. 8. Passing Information

While PO2 treats the EC's interruption as a request to notify the fire brigade, PO3 says "we've dropped it through, we have" (Figure 8:2). The EC seems doubtful, looking first at the inject on the table, then PO3, prompting FA1 to confirm that other agencies have been informed: "yeah" (Figure 8:3). This somewhat confused exchange actually indexes the absence of technologies. Normally, other agencies would automatically be notified through shared information systems and the police officers' answers indicate that they had assumed the exercise to simulate such infrastructures. The EC's interruption makes them realize that this is not the case: "but you want us to go to tables and tell people?" (PO3 Figure 8:3). This is keenly confirmed by the EC: "yes, because then that can trigger their injects." This is followed first by silence from the police officers, then activity. While PO2 gathers which information "they need to know" (Figure 8:4), PO3 clears his throat and markedly glances at him. It is not entirely clear whether this glance is a "raised eyebrow," but the silence that precedes it and subsequent activities suggest this. After the EC describes what he is asking of them as a matter of passing information "as you normally would … from your control room to their control room" (Figure 8:6), he walks out of earshot,

eagerly watched by PO2, who then enacts an exaggerated manual passing of information, saying "y'know," laughing (Figure 8:7). PO1 smiles, but walks across to the A-District fireservice control room, announcing: "I'm chief inspector Smith from A-District police control room," reading off the injects:

> "Err we have an operation Plato[12]. Multiple suspects are firing automatic weapons. Erm, (there's) casualties. A vehicle has been driven into the front of the airport and is on fire. There are also sounds of explosions coming from within the building. Possibly hand grenades. All available fire arms officers are being deployed to the area. We are setting up an outer cordon (.) when we get sufficient officers. At the moment we are struggling to stretch our resources. OK? Erm, we're looking to get you to an RV ((rendez-vous)) point as soon as possible but not to be deployed at the scene immediately. (.) Alright?" (Transcript from video 24th April 2012)

Following the information here initially entails shadowing the physical movement of injects, but then the ethnographer's attention and her camera are drawn to the micro-mobilities of these documents and information mobilized around them. She follows utterances, annotations, pointing gestures and glances, observing how information from injects enters into logs and is passed to other agencies. The transcript of two minutes from the beginning of the exercise highlights diverse flows of information that are further followed throughout the exercise, from situation reports to information about standard procedures, stories about personal roles and career, exercise "mechanics" and documentary evidence of individuals' conduct in a simulated crisis situation – reaching from earnest seriousness (PO1), to subtle irony (PO3), restraint (FA1), and cheeky humor (PO2). In addition, we gain insight into taken-for-granted "invisible" information infrastructures.

Analysis of observations from shadowing some of these flows over the full day of the exercise revealed friction between the agencies involved. It is beyond the scope of this paper to discuss these in detail, but several examples already surface in these first few minutes. Firstly, the fact that for each emergency service there are several teams – sometimes one in each area (A, B, and C-District) – results in duplication of roles in the command and control structure. It is unclear "who is running this." Secondly, standard plans and procedures have to be translated into situated action [Suchman 2007]. For example, the fact that "all available fire arms officers are being deployed to the area" from different police stations in the wider region might require a three way conversation between the three different police control rooms as well as the standard "joint command facility" three way communication between the different

[12] Operation Plato is a codename for "the possibility of indiscriminate shooting by terrorists for a period of time within a public arena causing mass casualties." [West Midlands Police 2012]

police, fire and medical emergency services. Thirdly, while in real world practice use of technologies can make it difficult to know what has or has not been communicated and to whom, here the absence of such technologies creates artificial information practices.

For practitioners and researchers alike, following information proved difficult in this context. By putting all the agencies who would normally be distributed across the region in one room, by removing technology, and by simulating expected responses that comply with standard procedures with a series of pre-prepared reports from fictitious incident sites, the exercise actually *dis*abled the responders' capacity to enact command and control structures and pass information between each other "as they would normally." This does not mean the exercise failed. On the contrary, exercises like this are important in improving interoperability between the different emergency response agencies. They generate occasions where responders from the different agencies meet and work together under exceptional, quite stressful, but also very social circumstances.

From shadowing information in such exercises we can learn how people trust and read each other. However, this exercise did not reveal much about the movement of information through digital circuits. An "Operation Plato" incident in the UK would, without doubt, spark intense intelligence gathering and analysis activities, utilizing CCTV at D-Town airport, and the Police National Computer (PNC). To better understand the practices involved, we carried out some participant observation and interviews with a police analyst (Thomas (T)), who demonstrated use of the PNC by embarking author (L) on a proto training session:

> We're sitting in front of his computer and Thomas says:
> T: What we are looking at now, only certain people are allowed into it and all access is monitored and recorded and if anyone is concerned about what I've done then professional standards will grab me and do a third degree[13] and I'll be disciplined or sacked if I've done anything inappropriate.
> L: Has that ever happened?
> T: Not to me. No but to others yes.
> L: What would something inappropriate be?
> T: Right, I've got access to certain areas of the police national computer. You have to be trained and pass a standard to get in. But if I've got access to PNC I could look at your criminal record, if you've got one. Is there a valid policing purpose? No. Why did I do it? Well I just wanted to- I'd lose my job for that. I may even be prosecuted or sent to jail. It's got to be a valid policing purpose. And that's not just valid in your own head, you know. I'm supposed to record a diary of every time I go in and record what I've done and why I did it but certainly I will get

[13] Idiom that describes "intense interrogation."

> e-mails periodically saying why am I doing this and if I don't come up with a proper answer to it- the police inspector in the midlands was it? He researched someone he thought was having an affair with his wife and he lost his job for it and then he killed his family and then himself … it's all incredibly tightly monitored. It's monitored nationally, it's monitored locally and the local monitoring will ask me to account and if they don't like what they hear they will go to professional standards so you just don't mess about.
> (Transcript of beginning of proto training session, June 2012)

This instructed glimpse into the PNC draws to attention how the use of personal data is regulated. Access privileges are restricted to "certain areas" and accountability is enforced by logs and inspectors. The Guardian's GCHQ source describes a similar auditing process for intelligence screening "to go back through the logs and see if it was justified or not" [in MacAskill et al. 2013]. In shadowing Thomas' entry into the PNC, we shadow these regulatory shadows and find ourselves in doubt over how effective such measures are. Unlike ethnographic shadows, the inspectors are an invisible presence, and they have power over the analysts, but their monitoring is based on the assumption that "justified or not" is a binary decision, when it is a contextual one. Yet, like the people whose records he might examine, Thomas has no way of knowing whether and when he is being scrutinized and how valid his contextual explanations might be perceived as. Monitoring has led to the discovery and prosecution of illegal use of PNC data by police investigators. Predominantly, these cases have been personally motivated misuse, such as the example Thomas describes. However, there have also been cases of misuse of power and social sorting, such as the use of "protester markers" during anti-war protests in the UK in 2005, which led to peaceful protesters being stopped, searched and obstructed [Lewis and Evans 2009]. Such misuse is rarely publicized or prosecuted and the monitoring measures fail to flag up such misuse, because the notion of "valid policing purpose" can be applied. The question whether such a purpose is legitimate and ethically and politically sound is difficult to address with these procedures. Following Thomas a short way into the PNC enables first hand experience of why analysts perceive the combination of an open data ocean and logging of their data access as both empowering and threatening. As pressures to share information with other category I and II responders grow in crisis management, concern over legal uncertainties is growing amongst police data analysts:

> "If the current legal framework regulating the sharing of information for the purposes of public protection is lawful, even in the face of criticism from the European Court of Human Rights, then an intolerable level of uncertainty as to the issue of that legality has now been reached." [Grace 2013, 29]

Retrospective go-alongs and interviews with emergency responders have shown us that in face-to-face interaction there is subtle but considerable control over legitimacy when sharing sensitive information. An ambulance doctor, for example, described how he would tell a police colleague to "wear gloves with that one" at the scene of an accident where victims are bleeding if a person the police needed to question was known to him as HIV positive, and police officers have described how they would instruct ambulance staff to "be careful with that one" if someone with a record of violent crime needed medical attention. Such euphemistic informational practices are highly economical and important to the safety of responders. They smoothly cross the boundaries between different agencies in an ephemeral way, avoiding explicitly disclosing personal information. But they rely on acute mutual understanding. Co-presence within the situation makes the statement intelligible, but more long term training of mutual understanding is also important. Exercises can help develop such understanding and trust, because they give participants opportunity to get to know others and practice different forms of communication. Such mundane, yet sophisticated practices of modulating the sensitivity of personal information in face-to-face interactions are difficult to transpose into digital information sharing, but it is precisely these practices that should be at the heart of alternative visions of informationalizing emergency services and other areas where data-based efficiencies are being sought.

6. Conclusion

By following the information it becomes clear that the analogy "data is the new oil" is vapid: data is not a raw material, resource or a fuel that can be extracted for human activity. Data is the ultimate renewable resource and making use of it is a process of cultivation not extraction [Thorp 2012]. But, if we extend the analogy to data spills, data dependence, and the deeply transformative effect oil has had on humanity and the planet – including fueling a "century of disasters" – important insights can be gained.

"How to follow the information?" is an important question for sociological research. As everyday life is turning digital, the fact that humans have never been "just" human but have always been entangled with technology in a "cyborg" co-existence [Heidegger 1977; Haraway 1990] takes on new significance. The convergence of the physical and the digital in human embodiment and "movement-space" [Thrift 2004] is changing what it means to be human. Informational mobilities are integral to these transformations. People create data – currently often imperceptibly – as part of

everyday living. Such data may be retained and be scrutinized – again imperceptibly and without the data subjects' knowledge. Innovation to enhance interoperability for the sharing and processing of personal data in crises is a particularly important site for the study of these transformations. It may be desirable for emergency responders to know as much as can be known from digital data about a person or population in a crisis but when does a crisis begin or end? Who decides? And how can sharing be controlled when the design philosophies that underpin innovation focus on direct interconnections between information systems, "one stop management," automation, and probabilistic techniques of analysis? With these technologies increasingly turned to prevention, social and political principles of privacy and solidarity are being transformed in ways that undermine fundamental values of equality and freedom.

"How to follow information?" is therefore also an important ethical and political question for innovation in practice, policy and technology. Technologies that make data sharing and analysis easier between the agencies involved in crisis management can spread beyond crises. Everyday technologies, technologies of marketing, surveillance and control, and crisis management are intricately connected. The design philosophies that shape them make their complexity, power and ubiquity invisible [Weiser 1991]. Through this, human sensory and social practices of modulating information disclosure are undermined. Some interaction designers are defining alternative design philosophies at this juncture, seeking ways of supporting people in transposing sensory and social practices into the hybrid digital and physical spaces where data are used, in "infrastructuring" and making computing more accountable or palpable [e.g. Karasti and Syrjänen 2004, Dourish 2001; Anderson et al. 2003]. New ways of "privacy by design," "accountable data-mining," and privacy preserving data sharing are taking shape [Langheinrich 2001; Weitzner et al. 2008; Agrawal and Ramakrishnan 2000].

A new politics of sociological method and new methods are needed to inform these alternative technological imaginaries and design philosophies. In this paper we have explored ways of following informational mobilities in the particular context of crises to show how tracking, going along with, tracing and shadowing information can reveal important aspects of social and material practices of mobilizing information. We have explored the contrast between friction-full and friction-less information practices. These studies enable a better understanding of informational mobilities and how they could play a productive role in more "agile" crisis response. But they also highlight conflicts between public and professional information models, and the different agencies brought together in crisis management. They illuminate the potential for location and communications data to inform preventive action, as well as some of the contentious and risky practices involved in this. Most importantly, we show how

technologies designed with the ambition to enable "direct interconnection," "one stop" access and "collect-all" ambitions in data oceans eliminate control for many data subjects. By following the information, the studies we have presented contribute to efforts that develop alternative design philosophies that actively support human sensory and social practices of making and making sense of data.

We thank our colleagues in the BRIDGE and SecInCoRe projects for inspiring discussion and input. This research is part of the BRIDGE Project, funded under the EU FP7 Security Theme, the EU FP7 project SecInCoRe and the UK EPSRC funded project Citizens Transforming Society: Tools for Change (CaTalyST).

References

Adey, P.

2009 "Facing Airport Security: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body." *Environment and Planning D: Society and Space* 27 (2): 274–295.

Agamben, G.

2005 *State of Exception*. Chicago: Chicago University Press.

Agrawal, R., and Ramakrishnan, S.

2000 "Privacy-preserving Data Mining." Pp. 439-450 in *Proceedings of the 2000 ACM SIGMOD international conference on Management of data (SIGMOD '00)*. New York, NY, USA: ACM.

Allen, D.K., Karanasios, S., and Norman, A.

2013 "Information Sharing And Interoperability: The Case of Major Incident Management." *European Journal of Information Systems*. Advance online publication doi:10.1057/ejis.2013.8

Amoore, L.

2006 "Biometric Borders: Governing Mobilities in the War on Terror." *Political Geography* 25: 336–351.

2011 "Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times." *Theory, Culture & Society* 28 (6): 24–43.

Anderson, C.

2008 "The End of Theory, Will the Data Deluge Make the Scientific Method Obsolete?." *Edge,* http://www.edge.org/3rd_culture/anderson08/anderson08_index.html [Accessed 25 February 2014].

Anderson, R., Brown, I., Dowty, T., Inglesant, P., Heath, W., Sasse, A.

2009 *Database State*. York: Joseph Rowntree Reform Trust.

Anderson, S., Hartswood, M., Procter, R., Rouncefield, M., Slack, R., Soutter, J., Voss, A.

2003 "Making Autonomic Computing Systems Accountable: The Problem of Human-Computer Interaction." *Proceedings of the 14th International Workshop on Database and Expert Systems Applications* (DEXA'03) 1529-4188, IEEE Computer Society.

Aradau, C., Lobo-Guerrero, L., Van Munster, R.

2008 "Security, Technologies of Risk, and the Political: Guest Editors' Introduction." *Security Dialogue* 39(2-3): 147–154.

Armstrong, H., Ashton, C., Thomas, R.

2007 "*Data Protection and Sharing – Guidance for Emergency Planners and Responders*. UK Cabinet Office London." www.cabinetoffice.gov.uk/media/132709/dataprotection.pdf [Accessed 15 August 2013].

Botero, A.

2013 *Expanding Design Space(s). Design in Communal Endeavours*. PhD Thesis: Aalto University Publication Series.

Boyd, D., Crawford, K.

2010 "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Information, Communication & Society* 15(5): 662–679.

Brown, I., Adams, A.A.

2007 "The ethical challenges of ubiquitous healthcare." *International Review of Information Ethics* 8: 53–60.

Bruni, A.

2005 "Shadowing Software and Clinical Records: On the Ethnography of Non-Humans and Heterogeneous Contexts." *Organization* 12 (3): 357–378.

Bu#scher, M.

2007 "Interaction in Motion: Embodied Conduct and Movement in Emergency Teamwork." In *Proceedings of the 2nd International Society for Gesture Studies Conference "Interacting Bodies"*, edited by L. Mondada, 15-18 June 2005, Lyon, France. http://gesture-lyon2005.ens-lyon.fr/article.php3?id_article=221

Bu#scher, M., and Mogensen, P.H.

2009 "Matereal Methods." Pp. 171-192 in *Ethnographies of Diagnostic Work: Dimensions of Transformative Practice*, edited by M. Bu#scher, D. Goodwin, and J. Mesman. London: Palgrave.

Bu#scher, M., Bylund, M., Sanches, P., Ramirez, L., and Wood, L.

2013 "A New Manhattan Project? Interoperability and Ethics in Emergency Response Systems of Systems." In *Proceedings of the 10th International ISCRAM Conference*, edited by T. Comes, F. Fiedrich, S. Fortier, J. Geldermann, and L. Yang, Baden-Baden, Germany, May 2013. ISCRAM.

Büscher, M., Urry, J., Witchger, K. (eds.)

2011 *Mobile Methods*. London: Routledge.

Castillo, C., Mendoza, M., Poblete, B.

2011 "Information Credibility on Twitter." *Distribution:* 675–684.

Cheong, M., Lee, V.C.S.

2010 "A Microblogging-based Approach to Terrorism Informatics: Exploration and Chronicling Civilian Sentiment and Response to Terrorism Events via Twitter." *Information Systems Frontiers* 13 (1): 45–59.

Committee of Public Accounts

2011 "The Failure of the FiReControl Project HC 1397." Public Accounts Committee - Fiftieth Report. London. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmpubacc/1397/139702.htm [Accessed 15 August 2013]

Corbin, J.M., Strauss, A.C.

1998 *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. London: Sage.

Crang, M, and Graham, S.

2007 "Sentient Cities: Ambient Intelligence and the Politics of Urban Space." *Information Communication Society* 10 (6): 789–817.

Dillon, M., Lobo-Guerrero, L.

2009 "The Biopolitical Imaginary of Species-being." *Theory, Culture & Society* 26 (1): 1–23.

Drabek, T.E., McEntire, D.A.

2002 "Emergent Phenomena and Multiorganizational Coordination in Disasters: Lessons from the Research Literature." *International Journal of Mass Emergencies and Disasters* 20(2): 197–224.

Defense Science Board (DSB)

2004 "Defense Science Board 2004 Summer Study on Transition to and from Hostilities." Washington. http://www.acq.osd.mil/dsb/reports/ADA430116.pdf [Accessed 15 August 2013]

Dourish, P.

2001 *Where the Action is*. Cambridge, MA: MIT Press.

Endsley, M.R.

1995 "Toward a Theory of Situation Awareness in Dynamic Systems." *The Journal of the Human Factors and Ergonomics Society* 37 (1): 32–64.

ENISA

2012 *Emergency Communications Stocktaking. A Study into Emergency Communications Procedures.* Brussels: European Network and Information Security Agency http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/emergency-communications-stocktaking/at_download/fullReport [Accessed 15 August 2013]

eScience

2012 *Earth Faces a Century of Disasters, Report Warns.* http://esciencenews.com/sources/the.guardian.science/2012/04/26/earth.faces.a.century.disasters.report.warns [Accessed 15 August 2013]

European Commission

2012 *Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.* Brussels: European Commission, 25.1.2012 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed 15 August 2013]

Furedi, F.

2006 *Culture of Fear*. London: Continuum International Publishing.

Gallagher, S.

2013 "Building a Panopticon: The Evolution of the NSA's XKeyscore. How the NSA went from Off-the-shelf to aHhomegrown 'Google for Packets'." *Ars Technica*. http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/ [Accessed 15 August 2013]

Gibbs, L.I., Holloway, C.F.

2013 *Hurricane Sandy After Action. Report and Recommendations to Mayor Michael R. Bloomberg.* New York. http://www.nyc.gov/html/recovery/downloads/pdf/sandy_aar_5.2.13.pdf [Accessed 15 August 2013]

Gjørv, A.B. (Ed.)

2012 "Rapport fra 22 Juli-Kommisjonen." Oslo. http://www.regjeringen.no/smk/html/22julikommisjonen/22JULIKOMMISJONEN_NO/EN/PRESENTATION_OF_THE_REPORT/PUBLICATIONS.HTM [Accessed 15 August 2013]

Grace, J.

2013 "Too Well-Travelled, Not Well-Formed? The Reform of Criminality Information Sharing In the UK." *The Police Journal* 86 (1): 29–52.

Graham, S.

2008 *Cities Under Siege: The New Military Urbanism*. London: Verso.

Graham, S., Marvin, S.

2001 *Splintering urbanism*. London: Routledge.

Haraway, D.J.

1990 "A Cyborg Manifesto." in *Simians, Cyborgs, and Women: The Reinvention of Nature*. London: Routledge.

Heaven, D.

2013 "Not Like us: Artificial Minds We Can't Understand." *New Scientist*, 8. August, 33–35.

Heidegger, M.

1977 *The Question Concerning Technology and other Essays*. New York: Garland Publishing.

Hine, C.

2007 "Multi-Sited Ethnography as a Middle Range Methodology for Contemporary STS." *Science, Technology & Human Values* 32(6): 652–671.

Introna, L.D.

2007 Maintaining the Reversibility of Foldings: Making the Ethics (Politics) of Information Technology Visible. *Ethics and Information Technology* 9(1): 11–25.

Jefferson, T.I., and Harrald, J.R.

2007 "Collaborative Technology: Providing Agility in Response to Extreme Events." *International Journal of Electronic Governance* 1(1): 79–93.

Johnson, B.

2012 "Taking Greater London Forward." *Mayoral Manifesto*. http://www.scribd.com/doc/91943852/Taking-Greater-London-Forward [Accessed 15 August 2013]

Johnston, P.

2007 "July 18 Police will get Access to Road Pricing Cameras." *The Telegraph*. http://www.telegraph.co.uk/news/uknews/1557789/Police-will-get-access-to-road-pricing-cameras.html [Accessed 15 August 2013]

Karasti, H., Syrjänen, A.L.

2004 "Artful Infrastructuring in Two Cases of Community PD." *Proceedings of the Eighth Conference on Participatory Design: ArtfulIntegration: Interweaving Media, Materials and Practices* 1: 20–30. New York, NY, USA: ACM.

Knight, K.

2013 *Facing the Future. Findings from the Review of Efficiencies and Operations in Fire and Rescue Authorities in England.* Her Majesty's Stationery Office. https://www.gov.uk/government/publications/facing-the-future [Accessed 15 August 2013]

Kraska, T.

2013 "Finding the Needle in the Big Data Systems Haystack." *Internet Computing IEEE* 17, (1): 84–86.

Landgren, J.

2005 "Supporting Fire Crew Sensemaking Enroute to Incidents." *International Journal of Emergency Management* 2(3): 176-182.

Langheinrich, M.

2001 "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems." Pp. 273-291 in *Proceeding UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing*.

Lazer, D., Pentland, A.S., Adamic, L., Aral, S., Barabasi, A.L., Brewer, D., Christakis, N., Contractor, N., Fowler, J., and Gutmann, M.

2009 "Life in the Network: The Coming Age of Computational Social Science." *Science* 323 (5915): 721-723.

Lesk, M.

2013 "Big Data, Big Brother, Big Money." *IEEE Security & Privacy* 11(4): 85–89.

Lewis, P., and Evans, R.

2009 "Activists Repeatedly Stopped and Searched as Police Officers 'Mark' Cars." *The Guardian*. http://www.theguardian.com/uk/2009/oct/25/surveillance-police-number-plate-recognition [Accessed 15 August 2013]

Lury, C., and Wakeford, N.

2012 *Inventive Methods: The Happening of the Social*. London: Routledge.

Lyon, D. (Ed.)

1994 *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

2002 *Surveillance as social sorting. Privacy risk and digital discrimination*. London: Routledge.

MacAskill, E., Borger, J., Hopkins, N., Davies, N., and Ball, J.

2013 "GCHQ Taps fFbre-optic Cables for Secret Access to World's Communications." *The Guardian*. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed 15 August 2013]

Macbeth, D.

1999 "Glances, Trances, and their Relevance for a Visual Sociology." Pp. 135-170 in *Media Studies: Ethnomethodological Approaches*, edited by P.L. Jalbert. Lanham, MD: University Press of America.

Maeda, Y. , Higashida, M., Iwatsuki, K., Handa, T., Kihara, Y., Hayashi, H.

2010 "Next Generation ICT Services Underlying the Resilient Society." *Journal of Disaster Research* 5(6): 627–635.

Mandate M/487

2013 "Mandate M/487 to Establish Security Standards Draft Report Phase 2 Proposed standardization work programs and road maps." http://www.cen.eu/cen/Sectors/Sectors/Security/citizens/Pages/default.aspx

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., and Byers, A.H.

2011 "Big data: The Next Frontier for Innovation, Competition, and Productivity." McKinsey Global Institute.

Marcus, G.E.

1995 "Ethnography In/of the World System: The Emergence of Multi-Sited Ethnography." *Annual review of anthropology* 24 (1): 95–117.

Mayer-Schönberger, V., and Cukier, K.

2013 *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin: Harcourt.

Mendonça, D.

2007 "Decision Support for Improvisation in Response to Extreme Events: Learning from the Response to the 2001 World Trade Center Attack." *Decision Support Systems* 43 (3): 952–967.

Naphade, M., Banavar, G., Harrison, C., Paraszczak, J., Morris, R.

2011 "Smarter Cities and their Innovation Challenges." *Computer* 44 (6): 32–39.

Oh, O., Agrawal, M., Rao, H.R.

2010 "Information Control and Terrorism: Tracking the Mumbai Terrorist Attack Through Twitter." *Information Systems Frontiers* 13 (1): 1–11.

Perng, S., Bu#scher, M., Halvorsrud, R., Wood, L.

2013 "Peripheral Response: Microblogging during the 22/7/2011 Norway Attacks." *International Journal of Intelligent Systems for Crisis Management* 5 (1). http://eprints.lancs.ac.uk/id/eprint/54012

Quarantelli, E.L.

1966 "Organizations Under Stress." Pp. 3-19 in *Symposium on Emergency Operations*, edited by R. Bricston, R. Santa Monica, CA: Systems Development Corporation.

Rauhofer, J.

2006 "Just Because You're Paranoid, Doesn't Mean They're Not After You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union." *SCRIPTed* 3 (4): 322–343.

Reding, V.
2012 "The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World." European Commission. http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/data-protection-reform2012_en.pdf [Accessed 15 August 2013]

Ribes, D.
2014 "Ethnography of Scaling, Or, How to a Fit a National Research Infrastructure in the Room." *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing:* 158–170.

Ruppert, E.
2012 "The Governmental Topologies of Database Devices." *Theory, Culture & Society* 29 (4-5): 116–136.

Savage, M., & Burrows, R.
2007 "The Coming Crisis of Empirical Sociology." *Sociology* 41 (5): 885–899.

Scheppele, K.L.
2003 "Law in a Time of Emergency: States of Exception and the Temptations of 9/11." *University of Pennsylvania Journal of Constitutional Law:* 1001-1083

Shapiro, D.
2005 "Participatory Design: The Will to Succeed." *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility:* 29–38.

Solove, D.J.
2004 *The Digital Person: Technology and Privacy in the Information Age*. New York: NYU Press.

Star, S.L.
1999 "The Ethnography of Infrastructure." *American Behavioral Scientist* 43 (3): 377–391.

Starbird, K., and Palen, L.
2013 "Working and Sustaining the Virtual "Disaster Desk." In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* - CSCW'13. New York: ACM Press.

Steenbruggen, J., Borzacchiello, M.T., Nijkampa, P., Scholten, H.
2013 "Data from Telecommunication Networks for Incident Management: An Exploratory Review on Transport Safety and Security." *Transport Policy* 28: 86–102.

Suchman, L.
2007 *Human-Machine Reconfigurations*. Cambridge: Cambridge University Press.

Suchman, L., Blomberg, J., Orr, J., Trigg, R.
1999 "Reconstructing Technologies as Social Practice." *American Behavioral Scientist* 43 (3): 392-408.

Tene, O., & Polonetsky, J.
2013 "Big Data for All: Privacy and User Control in the Age of Analytics." *Northwestern Journal of Technology and Intellectual Property* 11 (5): 239-273.

Thorp, J.
2012 "November 30. Big Data Is Not the New Oil." *Harvard Business Review.* http://blogs.hbr.org/2012/11/data-humans-and-the-new-oil/ [Accessed 16 March 2014]

Thrift, N.

2004 "Movement-Space: The Changing Domain of Thinking Resulting from the Development of New Kinds of Spatial Awareness." *Economy and Society* 33 (4): 582–604.

2005 *Knowing Capitalism*. London: Sage.

Tulich, T.

2012 "A View Inside the Preventive State: Reflections on a Decade of Anti-Terror Law" *Griffith Law Review* 21 (2): 209-243.

Urry, J.

2007 *Mobilities*. Cambridge: Polity.

2013 *Societies Beyond Oil: Oil Dregs and Social Futures*. London: Zed Books.

Vieweg, S., Palen, L., Liu, S.B., Hughes, A.L., Sutton, J.

2007 "Collective Intelligence in Disaster: Examination of the Phenomenon in the Aftermath of the 2007 Virginia Tech Shooting." In *Proceedings of the 5th International ISCRAM Conference* – Washington, DC, USA, May 2008, edited by F. Fiedrich and B. Van de Walle.

Watkins, T.

2011 "Norwegian Islander Ferries Children to Safety." *CNN*. http://edition.cnn.com/2011/WORLD/europe/07/22/norway.rescue.worker/index.html [Accessed 15 March 2014]

Weiser, M.

1991 "The Computer for the Twenty-First Century." *Scientific American* 265 (3): 107–114.

Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., and Sussman, G.J.

2008 "Information Accountability." *Communications of the ACM* 51 (6): 82–87.

West Midlands Police

2012 "Operation Plato – Update." Report of the Chief Constable.

Whalen, J.

1995 Expert Systems Versus Systems for Experts: Computer-aided Dispatch as a Support System in Real-world Environments. Pp. 161-183 in *Social and Interactional Dimensions of Human-Computer Interfaces,* edited by P. Thomas. Cambridge: CUP.

Yar, M.

2003 "Panoptic Power and the Pathologisation of Vision: Critical Reflections on the Foucauldian Thesis." *Society* 1 (3): 254–271.

Zedner, L.

2010 "Security, the State, and the Citizen: The Changing Architecture of Crime Control." *New Criminal Law Review* 13 (2): 379-403.

How to follow the information?

A Study of Informational Mobilities in Crises

Abstract: This article discusses mobile methods of "following the information" to contribute to a new politics of sociological method and inform the development of new design philosophies for information technologies. The approach is motivated by the increasing informationalization of everyday life in general and crisis management in particular. At this juncture social and political principles of privacy and solidarity are being transformed in ways that undermine fundamental values of equality and freedom. Crisis management is a particularly important site for such transformations. By showcasing different ways in which we have followed information in different crisis management settings through tracking, retrospective go-alongs, shadowing and tracing, we show how technologies designed with the ambition to enable "direct interconnection," "one stop" access and "collect-all" ambitions eliminate control for many data subjects. The studies we present contribute to alternative information system design philosophies that actively support human sensory and social practices of making and making sense of data.

Keywords: Informationalization, crisis management, mobile methods, privacy, social sorting.

Dr. **Monika Büscher** is Director of the Mobilities.lab, Centre for Mobilities Research, and Senior Lecturer in the Department of Sociology, Lancaster University, UK. She studies everyday practices of (im)mobility, making and making sense of information, place-making, distributed collaboration, collective intelligence. Post-human IT-ethics and phenomenology play a major part in her work. Her approach is ethnographic and analytically rooted in ethnomethodology, science and technology studies, mobilities research and phenomenology. Her work critically informs collaborative socio-technical innovation in different settings (from art and architecture to emergency response). She edits the book series *Changing Mobilities* with Peter Adey.

Dr. **Michael Liegl** is Senior Research Associate at Lancaster University. In his research he investigates the interplay of technology, spatial organization and social relations with a focus on the layering and hybridization of online and offline collaboration using (video-)ethnography and STS. He pursued this interest in research on digital urban art collectives, freelance nomadic work practices and location based social networks such as the GPS enabled smartphone dating app grindr. Currently, he engages in domain analysis and participatory design as well as in the exploration of social, legal and ethical implications of IT supported emergency response in EU 7FP funded BRIDGE project http:/bridgeproject.eu/en. Recent publications include: *Digital Cornerville* [Lucius & Lucius 2010], and "Nomadicity and the Care of Place" [*Journal of CSCW* 2014] and *Media Assemblages* [distinction 2014].

Dr. **Shaun Perng** is a Postdoctoral Researcher on the Programmable City project, exploring practices of incorporating codes and mobile technologies into everyday life in Dublin and Boston. He obtained his PhD from Sociology Department at Lancaster University on the topic of mobilities and changing everyday practices. Before joining NIRSA in 2013, he participated in the BRIDGE project, examining new opportunities and tension when incorporating citizens and social computing into emergency response. He was also a team member of an impact study of FutureEverything on how digital and locative arts challenges and changes Manchester and event participants.

Dr. **Lisa Wood** trained and worked as a therapy radiographer prior to completing her Masters in Health Research and her PhD in Science and Technology Studies (Lancaster). She has previously worked on research projects exploring working patterns of radiographers and the training of sonographers in the NHS. She has been a representative on the board for Lancaster University's Centre for Science Studies since 2010 and the Centre for Mobilities Research since April 2013. She worked as a Senior Research Associate in Lancaster's Sociology department before joining Lancaster Medical School as a lecturer in Social Sciences and also co-director of Year 3. Her research interests focus around technologically mediated practices drawing on Science and Technology Studies, Organisation Studies and Feminist Technoscience. She is interested in how practitioners generate knowledge, more recently looking at practices "on the move." This feeds into her interests in accountability, responsibility and autonomy in practice.